

Detecting Red Flag of Workplace Crime Using Mobile Data on Abnormal Usage Activities

Yuting Wang
School of Management
University of Science and Technology of China
yutingw@mail.ustc.edu.cn

Hefu Liu
International Institute of Finance, School of
Management
University of Science and Technology of China
liuhf@ustc.edu.cn

Ling Xue
J Mack College of Business and Economics
Georgia State University
lxue5@gsu.edu

Zhao Cai
Nottingham University Business School China
University of Nottingham Ningbo China
zhao.cai@nottingham.edu.cn

Abstract

The purpose of this paper is to investigate how to detect the workplace crime of organizational sales representatives (e.g., sales who work with external customers) through abnormal activities that can be traced by mobile devices and applications. The guardianship capability of organizations is considered as the moderator influencing the monitoring of abnormal usage activities calculated by deep learning. In this study, we conduct event history analysis on the occurrence of workplace crime utilizing a longitudinal panel data set, which comprises 197179 weekly observations in 3 years (2017-2019). Our finding provides evidence that the abnormal activity pattern is an effective signal for identifying workplace crimes. Furthermore, we illustrate how to design monitoring modes based on guardianship capability in order to maximize the effectiveness of mobile monitoring in reducing workplace crimes.

1. Introduction

Workplace crime (e.g., accepting kickbacks and stealing from organizations) has been recognized as a salient issue detrimental to organizations, especially considering sales representatives who operate at the boundary of an organization [1]. These employees possess elevated privileges and have more chances to exchange information, capital, and power with external stakeholders, which facilitates the occurrence of workplace crime [2, 3]. It is reported that most employees have personally observed or have firsthand knowledge of workplace crimes within their organizations during the past 12 months [4]. The

Association of Certified Fraud examiners estimated that workplace crimes cost American firms about \$3.5 billion annually [5]. Besides the enormous economic loss, workplace crime further tarnishes the organization's image, harms its reputation, and even leads to business failure [6]. These significant issues motivate the development of effective preventive solutions to reduce workplace crimes.

Scholars have suggested that IT monitoring can be effective in preventing workplace crimes [7]. For example, Scott, Balthrop [7] argued that electronic monitoring technologies can reduce illicit agent (e.g., frontline worker) behavior. Pierce, Snow [8] reported that the adoption of monitoring technology at a restaurant chain reduced sales representatives' theft. IT monitoring has garnered the attention of researchers in recent years, with studies focusing on whether it works or not [9]. However, few studies illustrate how to leverage IT monitoring to detect and reduce workplace crimes. Routine activity theory (RAT) was developed to understand the occurrence of crime and adapted to various contexts [10]. RAT suggests three conditions for crime to occur: a motivated offender, an opportunity in terms of a suitable target, and the absence of a capable or moral guardian. Schultz [11] suggests that behavioral cues, including employees' unusual behavior, correlated usage patterns, and personality traits can signal employees' propensity of being a motivated offender. With the growing forensic and detective capabilities enabled by IT and the greater availability of mobile technology, the recorded activities of employees are extended to ample contextual dimensions. The usage activity is enriched from simple used or not to visual, descriptive, and geographical aspects [12]. Therefore, the first goal of our study is *to investigate how abnormal usage activities traced by mobile apps are associated*

with the occurrence of workplace crime. To detect abnormal activities, we use Multilayer Perceptron (MLP) as a machine learning approach to learn the normal patterns of usage activities and compared them with the recorded patterns of activities.

According to RAT, the occurrence of workplace crime would be leveraged under difference level of guardianship [13]. Organizations need to implement both internal guardianship and external guardianship in monitoring sales representatives. Specifically, internal guardianship allows organizations to monitor sales representatives' internal collaboration with their colleagues, and external guardianship represents surveillance on sales representatives' interactions with external stakeholders. To assess the levels of guardianship, we define internal guardianship capability and external guardianship capability, which are measured by recorded guardianship subtracting learned normal guardianship. The literature has generally lacked empirical investigation of the impacts of internal and external guardianship capability in effect on workplace crime. Therefore, the second goal of our study is *to explore how organizations' guardianship capability influences the relationship between their abnormal usage activities that can be detected in mobile monitoring and their crime.*

Our empirical investigation is built upon the mobile IT usage data of sales representatives in a major Chinese manufacturer of liquor products. Sales representatives traveled to visit downstream partners (i.e., retailers), and they used mobile apps to record their trips. We aggregated data at the week level, which entails 197,179 observations about 1,822 Sales representatives in three years (2017-2019). The mobile usage activities include the uploading of visit locations, picture records, and log text. We used a deep learning method to identify the abnormal usage activities of uploading, which are based on the divergence between the reported activities and the normal activities learned from the deep learning model. We collected 210 workplace crime events identified by the company. Workplace crime is defined as the deliberate actions taken by employees to deceive, con, swindle, or cheat the company [14]. We also measured guardianship capabilities using the firm's internal and external surveillance times. Survival analysis is used to investigate the relationship between the sales representatives' mobile usage activities and workplace crimes and how this relationship is dependent on the firm's guardianship capabilities.

This study makes three theoretical contributions. Firstly, it illustrates how the abnormal patterns in mobile usage activities can be used as a crucial clue for detecting workplace crime. Second, the study considers how different types of self-reporting behaviors that are traced by mobile applications may have different

implications for workplace crime detection. Third, our study also illustrates how the consideration of internal and external guardianship capabilities may facilitate workplace crime detection using mobile monitoring data. This paper attempts to scrutinize how the abnormal information upload is shaped by guardianship capability, thereby offering insights into how to monitor Sales representatives based on the level of guardianship needed to maximize the monitoring effect on reducing workplace crime in the company.

2. Literature review and hypotheses development

2.1. Workplace crime and routine activity theory

Workplace crime has been defined as behaviors committed against organizations for the benefit of the individual perpetrator and might include embezzlement or padding expense reports [14]. It is reported that employee who works outside the company are usually at high risk of illicit behavior [15, 16]. In fact, it is reported that 60 percent of all employees engage in theft: 30 percent when presented with an opportunity to steal and 30 percent when they have found a way to steal after actively searching for an opportunity [17]. Employee theft and fraud are widespread problems in firms, with workers stealing roughly \$200 billion annually from U.S. firms to supplement their income which ruin the reputation and performance of the firm. [18]. More and more employees use their connections, power or access to resources available within the workplace in order to engage in informal economic activities outside it. Hence, the necessity of preventing the occurrence of workplace crime is crucial because of the growing business concern over client confidence, staff morale and deviant behavior [19, 20].

As a well-established criminological theory, RAT has attracted significant interest in criminology and has been subjected to numerous empirical studies. RAT provides a simple analytical framework, which allows straightforward applications in a variety of criminal activities. The theory asserts that there are three necessary components in a situation in order for a crime to occur: a suitable target, a lack of a capable guardian, and a motivated offender [10]. In other words, the theory asserts that if a motivated offender is presented with a suitable target that is not properly guarded against victimization, a crime is likely to occur. Its clear guidance allows for the development of policies and crime prevention initiatives [21]. RAT has been used to explain various crimes, from burglary [10], automobile theft [22] to cybercrimes [21].

This theory postulated that changes in the structure of the patterns of daily activity of people in cities following World War II could explain the rise in crime according to leading studies at the time. In the workplace situation of our paper, sales representatives face sufficient capital and have offsite opportunities. These accessibility enables them to get to the target and then leave the crime's scene easily. Hence, the potential motivated offender is seen as the employee who performed abnormal behavior in their routine mobile usage work. The suitable target is the pecuniary and relational resources the sales representatives can get access to, for example, the retailers utilize bribes to trade the resources of the organization with sales representatives. The capable guardian represents the guardianship capability that the organization exerts on sales representatives.

2.2. Abnormal usage activity

The extant literature has considered utilizing auditing and encouraging whistleblowing to reduce workplace crime [23, 24]. However, by the time the crime is discovered, the money is unrecoverable, or the chance to recover the total amount of the loss is very limited. Furthermore, it is costly and time-consuming to investigate workplace crime especially involving large-scale multinational operations. If the focus is on workplace crime pre-detection of monetary losses, time and effort to reconstruct fraudulent transactions, track down the perpetrator, and reclaim missing funds can be saved. An abnormal and significant change in behavior can signal a negative outcome [25]. In routine activities, unusual absences or timekeeping such as frequent sick days or unexpected half-days taken can indicate that the staff member has something else on the mind. The employee looking for an excuse to linger at work to be alone could pose a problem [26]. Also, unusual financial reporting patterns and unusual transactional behaviors are proven as an effective way to detect the occurrence of deviant behavior [27, 28].

With the availability of information technologies, abnormal usage behavior such as upload, log, and access attempts can be tracked as a signal fraud problem [26]. Organizations expend substantial resources to monitor sales representatives, and that much of this monitoring activity is intended to record their deviations from workplace norms [29, 30]. Mobile technology empowers the firm to monitor sales representatives with substantial detailed activity recorded anytime and anywhere. Based on different dimensions of the mobile recorded information, we categorized the activities monitored by the mobile technology as photo uploads, log text uploads, and location uploads [12]. Photo uploads reflect the number of digital photographs taken

with a camera phone and sent back to the focal company, which contains sales representatives' selfies in the working environment. Log text uploads reflect the text content that sales reps used to describe their work (during visits to downstream partners) and upload words through the mobile application, which helps the company track the progresses of their work. Location uploads reflect the actual geographic positions that sales representatives visited. The abnormal activities are measured by the differences between the actual uploads of the content (i.e., photos, text logs, and locations) and the normal patterns of uploading learned in a deep learning model.

3. Hypotheses development

Location uploads are the fundamental report of sales representatives, which is easy and flexible to modify. When sales representatives perform differently in uploading locations, on the one hand, they tend to hide their guilty by showing hard-working through active location uploads. On the other hand, they would like to be invisible in the company by low frequent uploading locations. The photo of the selfie and the log text contains much more information and hard to modify than the location report. As complementary information, log text and photo are usually uploaded randomly based on contingencies of the external environment, which is unstable and unpredictable. Compared with the abnormal pattern, sales representatives who perform the normal photo and log text pattern usually suffer a higher possibility of beautifying their behavior by routinely controlling the uploading. They design a stable work process by reporting the photo and log text in a specific pattern. The deliberate, consistent behavior represents the abnormal signals of deviant behavior. Hence, abnormal change of the photo and log text uploads can be seen as the effective monitoring mode in reducing workplace crime. Hence, we propose the following.

H1: Abnormal location uploads are positively associated with the likelihood of workplace crime.

H2: Abnormal photo uploads are negatively associated with the likelihood of workplace crime.

H3: Abnormal log text uploads are negatively associated with the likelihood of workplace crime.

Internal guardianship capability represents the organizations' surveillance of sales representatives' internal activities. When the organizations exert higher internal guardianship capability, sales representatives communicate with their colleagues with great caution, representing them more carefully with their routine work [31]. Also, the separated information can be gathered during the communication. Hence, the positive detection of abnormal location uploads will be weakened by higher internal guardianship capability.

On the other hand, their understanding of the organization's strategic decisions and resource allocation is improved by monitoring their operational process, which helps them better beautify their behaviors to satisfy the requirements of organizations. With such knowledge, the relationship between abnormal photos, log text uploads, and workplace crime is weaker. Hence, we propose the following hypotheses:

H4a: With higher internal guardianship capability, the relationship between abnormal location uploads and workplace crime is weaker.

H4b: With higher internal guardianship capability, the relationship between abnormal photo uploads and workplace crime is weaker.

H4c: With higher internal guardianship capability, the relationship between abnormal log text uploads and workplace crime is weaker.

Sales representatives in the inter-organization relationship are the external representations of the company [32]. External guardianship capability is defined as the extra guardianship times compared with the usual guardianship. When organizations exert more external guardianship, sales representatives can build a strong network with the organization's collaborators through frequent visits [33]. The autonomy of sales representatives is enhanced by performing extra external representations. Under a higher autonomy level, the identification of the sales representatives will be reduced [34]. They tend to perform opportunistically since they can make friends autonomously. Hence, the positive relationship between abnormal location uploads and workplace crime is strengthened; the negative relationship between abnormal photo, log text uploads, and workplace crime is weakened. We propose the following hypotheses:

H5a: With higher external guardianship capability, the relationship between abnormal location uploads and workplace crime is stronger.

H5b: With higher external guardianship capability, the relationship between abnormal photo uploads and workplace crime is weaker.

H5c: With higher external guardianship capability, the relationship between abnormal log text uploads and workplace crime is weaker.

4. Methodology

We collaborated with a Fortune Chinese 500 manufacturer, referred to as the "*G Company*" hereafter.

We collected sale representatives' mobile uploading data from G Company's database, gathering 1822 sale representatives' mobile self-report information from 1/8/2017 to 6/23/2019. The sample consists of 197,179 observations. Through our interview with the human source manager of G Company, we were informed that workplace crime has cost the company millions of dollars every year, which showed the importance of reducing workplace crime [17].

4.1. Dependent variables

We defined workplace crime as deliberate actions taken by employees to deceive, con, swindle, or cheat the company or other vital stakeholders [14]. Workplace crime is a repeated event for some employees. We included all workplace crime events and used repeated survival analysis to model this complicated relationship. To measure workplace crime, we collected the relevant files of the employees from the company announcement and recognized 210 workplace crime events. In the announcement, it includes when the employees do workplace crime and when the company catches them for doing so. Workplace crime in the announcement includes fake expense application announcement, unreasonable application announcement, and unreasonable product price announcement. All the workplace crime is seen as the benefits stealing from the focal company. We marked the application date as the workplace crime date for the application that had a specific date. For the workplace crime we did not know the specific date, through the interview, we used one month before the announcement as the workplace crime date as the manager suggested. The longer the time until the occurrence of workplace crime means the lower likelihood of workplace crime. The shorter the time to the occurrence of workplace crime represents the higher workplace crime likelihood.

4.2. Calculating abnormal usage activities and guardianship capability

This study offered a calculation of the main ANN model that has been shown to be useful in time series forecasting, as well as a standard procedure for the practical application of ANN in this type of task. The model analyzed is the Multilayer Perceptron (MLP).

Table 1. Description of Variables

Variable	Dimension	Measurement
Dependent variable	Workplace Crime	Binary indicator for the week of doing workplace crime, set to 1 for workplace crime.
Moderator	IGC	Internal Guardianship _{iweek} – Learning Internal Guardianship _{iweek}
	EGC	External Guardianship _{iweek} – Learning External Guardianship _{iweek}
Independent variables	ALU	ABS[Location Uploads _{iweek} – Learning Location Uploads _{iweek}]
	APU	ABS[Photo Uploads _{iweek} – Learning Photo Uploads _{iweek}]
	ATU	ABS[Text logs Uploads _{iweek} – Learning text logs Uploads _{iweek}]
Control variable	Age	The number of years since sale representatives born
	Experience	The number of years since sale representatives join sales department
	Marriage	1 for the sale representatives in marital status, 0 for the sale representatives who are single
	Gender	Male for 1, female for 0

Note: 1. * shows significance at the 0.05 level, ** shows significance at the 0.01 level, and *** shows significance at the 0.001 level.
2. ALU: Abnormal location uploads APU: Abnormal photo uploads ATU: Abnormal log text uploads IGC: Internal Guardianship Capability EGC: External Guardianship Capability

MLP is used to train and predict normal activities and normal coordination. We took their characteristics, such as marriage, gender, age, experience, hire source and education as predicted features. Also, time features such as year, month, and day are added to the model. In this paper, k-fold training method is used to save the prediction result of each training, and the final evaluation result is obtained by taking the average value. K-fold improves the robustness of the prediction results and better evaluates the prediction ability of the model. By grid search method, it is found that the optimal parameter of MLP is hidden_layer_Sizes (one hundred, fifty), activation is ReLu, solver is Adam, alpha is 0.01, max_iter is 50, learning_rate_init = 0.001. To identify the level of accuracy in the prediction, MAPE value (Mean Absolute Percentage Error) of each variable is tested less than 100.

Abnormal usage activities. We measured abnormal location uploads (ALU) as an absolute value of the times of uploading locations recorded in the APP in current week minus the learning times in this week. The abnormal photo uploads (APU) are tested as the absolute value of the times of uploading selfies in the app in the current week minus the learning selfie uploads. The abnormal log text upload (ATU) refers to the absolute value that times of word uploads in the current week minus the times learned in this week.

Guardianship capability. Internal guardianship refers to the times organization monitoring the employees when they process internal work with their colleagues. External guardianship is defined as the times of organization monitoring the employees when they

build network with external collaborators. The guardianship of internal and external capability was measured by the times of guardianship in the current week minus the learning times.

The control variables used in our analysis were identified from prior research on employee-level study. First, the employee's age, we used the age of each employee according to weekly observation. We use the dummy variable to test the gender and the marital status of the employee.

Experience was measured by the years since they joined the sales company, which change with the weekly observation. Summary statistics and bivariate correlations are provided in Table 1 and Table 2.

5. Statistical approach

In this study, we used survival analysis, and also called Event history analysis, to model employee's workplace crime in the mobile monitor setting. We utilized a repeated-events Cox proportional hazards with robust employee-level standard errors approach to estimate the workplace crime rates of employees [35, 36]. Hazard models are especially suited for duration data as they take a right censoring into account [37] and allow time-varying measures of variables [38]. Compared to a binary-choice model that only takes a (0,1) outcome into account, the hazard model considers additional information such as detailed survival times and censoring. Hazard models thus offer greater stability and predictive accuracy for duration data [39].

Given these advantages, a number of studies have relied on hazard models to analyze duration relationship [40].

Table 2. Correlation of Variables for Research Model

	Mean	Std. dev.	1	2	3	4	5	6	7	8	9
ALU	3.786	5.596									
APU	5.310	6.737	0.384**								
ATU	2.974	4.989	0.172**	0.319**							
IGC	-0.521	3.891	0.048**	0.009**	0.010**						
EGC	5.989	0.517	-0.059**	-0.141**	-0.156**	-0.011**					
Age	33.36	7.312	-0.043**	-0.058**	-0.057**	0.001	0.111**				
Experience	6.77	49.486	-0.014**	-0.019**	-0.024**	0.001	0.965**	0.083**			
Marriage			-0.003	-0.006**	-0.012**	0.003	-0.031**	0.025**	-0.036**		
Gender			-0.008**	-0.003	0.000	0.001	-0.004	0.001	-0.004	0.112**	
Fraud			0.003	-0.004	-0.006**	0.011**	0.000	-0.005*	-0.001	0.004*	0.003

Note: 1. * shows significance at the 0.05 level, ** shows significance at the 0.01 level, and *** shows significance at the 0.001 level.
2. ALU: Abnormal location uploads APU: Abnormal photo uploads ATU: Abnormal log text uploads IGC: Internal Guardianship Capability EGC: External Guardianship Capability

Also, PH model enables us to incorporate dynamic effects of variables on survival time through the inclusion of time-dependent covariates in an extended Cox model [41]. To accommodate our time-varying covariates, we aggregated our data into weekly periods and estimated employee's workplace crime probability at the end of each period. The CoxPH model assumes proportional hazards, and such heterogeneity is a threat to this assumption [42]. We tested for the proportional hazards and found that our models satisfied this assumption.

We used Prentice, William and Peterson model (PWP - GT) to handle repeated workplace crime, which accounts for repeated workplace crime, which describes an intensity process from the occurrence of an immediately preceding event, with the gap time defined as $(t - t_{k-1})$. PWP approaches are conditional models as an individual is not considered in the risk set for the k th event until experiencing the $(k-1)_{th}$ event [43]. Following the idea described above, the model is defined as:

$$\lambda_{ik}(t) = \lambda_0(t - t_{k-1}) \exp \{ \beta_k x_i(t) \}$$

Specially, the estimated robust standard errors were clustered by the employee, each strata (workplace

crime) had its own baseline hazard rate of ending in workplace crime, and each observation (employee) was not at risk for a later event (first workplace crime) before all earlier events (first and second workplace crime) have occurred [36]. Also, rather than stratifying the data using the number of workplace crime, we used a continuous variable to control for the number of workplace crime. This has the advantage of controlling for occurrence dependence [44].

6. Results

Table 3 reports the maximum likelihood coefficient estimates and hazard ratio estimates of the survival analysis using a Cox proportional hazards model in R [45]. In Column 1 of Table 3, we presented a baseline model specification where we included only the control variables in the model. In the second column, we added three independent variables into the model.

Table 3. Cox Proportional Hazard Model

	Variables	Model 1	Model 2	Model 3	Model 4
	Age	-0.02464(0.027)	-0.023 (0.027)	-0.023 (0.027)	-0.027 (0.026)
	Gender	0.314(0.268)	0.317 (0.268)	0.315 (0.268)	0.320 (0.268)
	BS experience	--0.0245(0.027)	-0.034 (0.027)	-0.047 (0.028)	-0.051 (0.024)
	Marriage	0.394(0.254)	0.387 (0.254)	0.386 (0.252)	0.386 (0.253)
H1	ALU		0.014*** (0.003)	0.011* (0.004)	0.008 (0.008)
H2	APU		-0.029* (0.014)	-0.020 (0.014)	0.076 (0.022)
H3	ATU		-0.055* (0.025)	-0.043 (0.029)	0.029 (0.037)
	IGC			0.065* (0.026)	0.054** (0.036)
	EGC			0.011 (0.009)	-0.012 (0.011)
H4a	ALU * IGC				-0.004* (0.001)
H4b	APU* IGC				0.006* (0.003)
H4c	ATU * IGC				0.001 (0.004)
H5a	ALU * EGC				-0.0001 (0.001)
H5b	APU * EGC				0.002* (0.001)
H5c	ATU * EGC				0.005** (0.001)
	χ^2	19.300***	36.140***	52.430***	69.300***
	AIC	3052.439	3041.602	3029.308	3024.438
	Observations	197179	197179	197179	197179
	Individuals	1822	1822	1822	1822
	Events	210	210	210	210
Note: 1. * shows significance at the 0.05 level, ** shows significance at the 0.01 level, and *** shows significance at the 0.001 level. 2. ALU: Abnormal location uploads APU: Abnormal photo uploads ATU: Abnormal log text uploads IGC: Internal Guardianship Capability EGC: External Guardianship Capability					

In Column 3, we presented a model that incorporates the moderator variables. For testing the moderation effects, in Column 4 we added 6 interactions into the model. In the main hypotheses tests, results are consistent with H1, H2, H3. In the moderation test, H4a, H4b, H5b, and H5c are supported by the results. While the H4c and H5a are not proved.

7. Discussion and implications

As mobile technology becomes a central feature of society, exploring mobile APP in monitoring employees is a key issue for IS researchers. By unraveling the relationship between abnormal usage activities monitored by mobile APP and the occurrence of workplace crime in boundary-spanning relationships,

this study makes three contributions. First, the critical role of mobile monitoring is confirmed by this research, which is essential to manage deviant employees and reduce illicit behavior. As elaborated by the literature, mobile technology affects critical functions of management, such as supervision and control, which evolve towards more open and mobile forms [12]. In addition to existing studies which point out control and whistleblowing as factors that weaken the occurrence of workplace crime [23, 46], this study proposes abnormal usage activities recorded by mobile APP as an effective approach and the red flag to eliminating workplace crime. These findings echo extant claims on the crucial role of monitoring employees and jointly creating value with the company [8].

Second, based on mobile technology features, this study scrutinizes the mechanism by calculating sales representatives' abnormal usage activities by deep learning. The sales representatives who perform abnormal location uploads behavior should be paid close attention to because they are more likely to commit workplace crimes. Third, we extend the ongoing discussion on the employee who works as the boundary of the organizations by scrutinizing organizations' guardianship to reduce their deviant behavior [15].

Third, this study extends the application of routine activity theory to understand the relationships in workplace crime. Consistent with RAT, the result shows abnormal usage patterns, and the presence of guardianship (i.e., internal guardianship capability and external guardianship capability) will influence the occurrence of workplace crime.

The findings of this study offer guidelines for the company. Managers should monitor employees on their abnormal usage activities. When designing the

monitoring mode of the boundary spanners, location monitoring is the critical approach to detect workplace crime. At the same time, the abnormal photo and log text uploads are the effective way to recognize the normal sales representatives. For the sales representatives who upload their locations abnormally, managers should pay attention to monitoring their internal work. For the sales representatives who upload their photo and log text abnormally, too much attention on their internal and external work will impede the practical inhibiting effect of abnormal photo and log text uploads.

8. Acknowledgement

This work was supported by the National Key R&D Program of China (2020AAA0103804) and the National Natural Science Foundation of China (NSFC: 71971202).

9. References

- [1] Vadera, A.K. and R.V. Aguilera, "The Evolution of Vocabularies and Its Relation to Investigation of White-Collar Crimes: An Institutional Work Perspective". *Journal of Business Ethics*, 2015. 128(1): p. 21-38.
- [2] Chapple, W., et al., "Lights Off, Spot On: Carbon Literacy Training Crossing Boundaries in the Television Industry". *Journal of Business Ethics*, 2020. 162(4): p. 813-834.
- [3] Mortensen, M. and M.R.J.O.S. Haas, "Perspective—Rethinking Teams: From Bounded Membership to Dynamic Participation". *Organization Science*, 2018. 29(2): p. 341-355.
- [4] Forensic, K., "Integrity Survey 2008–2009". New York, NY: KPMG LLP, 2008.
- [5] Mathew, S.K., *You Just Got Cheated: Understanding White-Collar Crime*. 2020: Sage Publications Pvt. Limited.
- [6] Van Akkeren, J. and S. Buckby, "Perceptions on the Causes of Individual and Fraudulent Co-offending: Views of Forensic Accountants". *Journal of Business Ethics*, 2017. 146(2): p. 383-404.
- [7] Scott, A., A. Balthrop, and J.W. Miller, "Unintended responses to IT - enabled monitoring: The case of the electronic logging device mandate". *Journal of Operations Management*, 2020. 67(2): p. 152-181.
- [8] Pierce, L., D.C. Snow, and A. McAfee, "Cleaning House: The Impact of Information Technology Monitoring on Employee Theft and Productivity". *Management Science*, 2015. 61(10): p. 2299-2319.
- [9] Scott, A., A. Balthrop, and J.W. Miller, "Unintended responses to IT - enabled monitoring: The case of the electronic logging device mandate". *Journal of Operations Management*, 2020.
- [10] Cohen, L.E. and M. Felson, "Social change and crime rate trends: A routine activity approach". *American sociological review*, 1979: p. 588-608.
- [11] Schultz, E.E., "A framework for understanding and predicting insider attacks". *Computers & security*, 2002. 21(6): p. 526-531.
- [12] Leclercq-Vandelannoite, A., H. Isaac, and M. Kalika, "Mobile information systems and organisational control: beyond the panopticon metaphor?". *European Journal of Information Systems*, 2014. 23(5): p. 543-557.
- [13] Luo, X.R., et al., "Why Individual Employees Commit Malicious Computer Abuse: A Routine Activity Theory Perspective". *Journal of the Association for Information Systems*, 2020. 21(6): p. 5.
- [14] Zahra, S.A., R.L. Priem, and A.A. Rasheed, "The Antecedents and Consequences of Top Management Fraud". *Journal of Management*, 2005. 31(6): p. 803-828.
- [15] Korschun, D., "Boundary-Spanning Employees and Relationships with External Stakeholders: A Social Identity Approach". *Academy of Management Review*, 2015. 40(4): p. 611-629.
- [16] Williams, P., "The Competent Boundary Spanner". *Public Administration*, 2002. 80(1): p. 103-124.
- [17] Thomas, J., "Prosecution of white-collar crime rising". *Chicago Tribune*, 1991. 10.
- [18] Litzky, B.E., K.A. Eddleston, and D.L. Kidder, "The Good, the Bad, and the Misguided: How Managers Inadvertently Encourage Deviant Behaviors". *Academy of Management Perspectives*, 2006. 20(1): p. 91-103.
- [19] Xu, Z., C. Cheng, and V. Sugumaran, "Big data analytics of crime prevention and control based on image processing upon cloud computing". *Journal of Surveillance, Security and Safety*, 2020. 1(1): p. 16-33.
- [20] Davis, B., D. Read, and S. Powell, "Exploring employee misconduct in the workplace: Individual,

- organizational, and opportunity factors". *Journal of Academic and Business Ethics*, 2014.
- [21] Leukfeldt, E.R. and M. Yar, "Applying routine activity theory to cybercrime: A theoretical and empirical analysis". *Deviant Behavior*, 2016. 37(3): p. 263-280.
- [22] Rice, K.J. and W.R. Csmith, "Socioecological models of automotive theft: Integrating routine activity and social disorganization approaches". *Journal of Research in Crime and Delinquency*, 2002. 39(3): p. 304-336.
- [23] Butler, J.V., D. Serra, and G. Spagnolo, "Motivating Whistleblowers". *Management Science*, 2020. 66(2): p. 605-621.
- [24] DeZoort, F.T. and P.D. Harrison, "Understanding Auditors' Sense of Responsibility for Detecting Fraud Within Organizations". *Journal of Business Ethics*, 2018. 149(4): p. 857-874.
- [25] Furnham, A. and J. Taylor, *The dark side of behaviour at work: Understanding and avoiding employees leaving, thieving and deceiving*. 2004: Springer.
- [26] Coenen, T.L., *Essentials of corporate fraud*. Vol. 37. 2008: John Wiley & Sons.
- [27] Ozili, P.K., "Advances and issues in fraud research: a commentary". *Journal of Financial Crime*, 2020.
- [28] Dorminey, J., et al., "The evolution of fraud theory". *Issues in accounting education*, 2012. 27(2): p. 555-579.
- [29] Dickens, W.T., et al., "Employee crime and the monitoring puzzle". *Journal of Labor Economics*, 1989. 7(3): p. 331-347.
- [30] Singh, T. and A. Johnston, "How much is too much: employee monitoring, surveillance, and strain". 2019.
- [31] Stamper, C.L. and M.C. Johlke, "The impact of perceived organizational support on the relationship between boundary spanner role stress and work outcomes". *Journal of Management*, 2003. 29(4): p. 569-588.
- [32] Huang, Y., et al., "An investigation of interpersonal ties in interorganizational exchanges in emerging markets: A boundary-spanning perspective". *Journal of Management*, 2016. 42(6): p. 1557-1587.
- [33] Schotter, A.P.J., et al., "Boundary Spanning in Global Organizations". *Journal of Management Studies*, 2017. 54(4): p. 403-421.
- [34] Richter, A.W., et al., "Boundary spanners' identification, intergroup contact, and effective intergroup relations". *Academy of Management Journal*, 2006. 49(6): p. 1252-1269.
- [35] Cox, D.R., "Regression models and life - tables" . *Journal of the Royal Statistical Society: Series B (Methodological)*, 1972. 34(2): p. 187-202.
- [36] Box-Steffensmeier, J.M., J.M. Box-Steffensmeier, and B.S. Jones, *Event history modeling: A guide for social scientists*. 2004: Cambridge University Press.
- [37] Helsen, K. and D.C. Schmittlein, "Analyzing duration times in marketing: Evidence for the effectiveness of hazard rate models". *Marketing Science*, 1993. 12(4): p. 395-414.
- [38] Nitzan, I. and B. Libai, "Social effects on customer retention". *Journal of Marketing*, 2011. 75(6): p. 24-38.
- [39] Bolton, R.N., "A dynamic model of the duration of the customer's relationship with a continuous service provider: The role of satisfaction". *Marketing Science*, 1998. 17(1): p. 45-65.
- [40] Jensen, M. and H. Kim, "The Real Oscar Curse: The Negative Consequences of Positive Status Shifts". *Organization Science*, 2015. 26(1): p. 1-21.
- [41] Bowman, D., "Survival models for marketing strategy". *Assessing Marketing Strategy Performance*, 2004: p. 115-144.
- [42] Grambsch, P.M. and T.M. Therneau, "Proportional hazards tests and diagnostics based on weighted residuals". *Biometrika*, 1994. 81(3): p. 515-526.
- [43] Thenmozhi, M., et al., "Survival analysis in longitudinal studies for recurrent events: Applications and challenges". *Clinical Epidemiology and Global Health*, 2019. 7(2): p. 253-260.
- [44] Heckman, J.J. and G.J. Borjas, "Does unemployment cause future unemployment? Definitions, questions and answers from a continuous time model of heterogeneity and state dependence". *Economica*, 1980. 47(187): p. 247-283.
- [45] Therneau, T., *A package for survival analysis in S. R package version 2.37-7*. 2014.
- [46] Yiu, D.W., W.P. Wan, and Y.H. Xu, "Alternative Governance and Corporate Financial Fraud in Transition Economies: Evidence From China". *Journal of Management*, 2019. 45(7): p. 2685-2720.